United States Department of Health & Human Services
Office of the Assistant Secretary for Administration and Management

U.S. Department of Health & Human Services

Handbook Guide For Personal Identity Verification (PIV) Implementation of Homeland Security Presidential Directive 12 (HSPD-12)

October 2005

(As of 4 October 2005)

TABLE OF CONTENTS

INTRODUCTION 3

1 PURPOSE 3
2 BACKGROUND 4
3 APPLICABILITY 5
4 SCHEDULES AND DEADLINES 7
5 ABBREVIATIONS 8
6 DEFINITIONS 10

PIV I 14

2.1 PIV I APPLICABILITY 14
2.2 PRIVACY POLICY 14
2.3 NACI/OPM/NS BI REQUIREMENTS 15
2.4 PUBLIC TRUST POSITIONS 16
2.5 REGISTRATION, IDENTITY PROOFING, & CREDENTIAL ISSUANCE 19
a. Roles and Responsibilities 19
b. Registration, Identity Proofing, and Issuance Procedures 20
c. Appeal Procedures for Denial of Credential 24
2.6 EXPIRATION DATE REQUIREMENTS 25
2.7 CASES WHERE PIV I DOES NOT APPLY 25
a. Replacement Credentials 25
b. Temporary Credentials 26
c. Visitor Credential 26
2.8 CONTRACTING IMPACTS 26
2.9 AUDIT & RECORDS MANAGEMENT 26
2.10 USE OF APPROVED FORMS 26
2.11 PHYSICAL ACCESS CONTROL SYSTEMS (PACS) 27
a. Continued Use of Existing PACS 27
b. Upgrading Existing PACS 27
c. Purchase of New PACS 27
2.12 LOGICAL ACCESS CONTROL SYSTEMS (LACS) 28
a. Continued Use of Existing LACS 28
b. Upgrading Existing LACS 28
c. Purchase of New LACS 28

PIV II 29

3.1 PIV II OVERVIEW 29
3.2 PIV II APPLICABILITY 30
a. Facilities 30
b. Information Systems 30

APPENDIX A 31

4.1 TRAINING 31
4.2 WHERE TO GET ASSISTANCE 31
4.3 REPORTING REQUIREMENTS 31
a. Number of PIV credentials issued during designated period 31
b. Number of PIV credentials cancelled during designated period 31
c. Number of PIV credentials replaced during designated period 32
4.4 PIV I PROCESS FLOW DIAGRAM 32
4.5 HSPD 12 DOCUMENT 32

CHAPTER 1

INTRODUCTION

1 ***PURPOSE***

The purpose of this Department of Health and Human Services (DHHS) Handbook is to provide guidance and procedures within the Department of Health & Human Services Staff Divisions (STAFFDIVS) and Operating Divisions (OPDIVS) where guidance does not exist, and to meet the Personal Identity Verification (PIV) requirements of Homeland Security Presidential Directive (HSPD) 12 and other directives or standards related to HSPD-12:

Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004

U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, dated February 25, 2005

Office of Management and Budget (OMB) Implementation Directive M-05-24, dated August 5, 2005

HSPD 12 mandates the development and implementation of a mandatory, government-wide Standard for secure and reliable forms of identification for all Federal employees and contractors for access to federally controlled facilities and information systems.

FIPS 201 defines a reliable, government-wide PIV system for use in applications such as access to federally controlled facilities and information systems. It also specifies a PIV system within which common identification credentials can be created and later used to verify a claimed identity.

OMB Implementation Directive M-05-24 provides guidance for implementing the requirements in FIPS 201 and HSPD 12. The guidance clarifies timelines, applicability, and the requirements of PIV I and PIV II.

For purposes of this Handbook, DHHS mission areas, agencies, and offices are collectively referred to as "Staff Division (STAFFDIV)" or "Operating Division (OPDIV)."

2 ***BACKGROUND***

In years past, government agencies have all required various levels and means of authenticating Federal employees and contractors as a requirement to enter government buildings and use government systems. Where appropriate, the agencies also implemented authentication mechanisms to allow access to specific areas or systems. The methods and level of assurance for authentication (i.e., identification) and authorization (i.e., permission) vary widely from agency to agency, and sometimes within a single agency.

HSPD 12 requires that all government agencies develop specific and consistent standards for both physical and logical identification systems. NIST's FIPS 201 establishes detailed standards on implementing processes and systems to fulfill the requirements of HSPD 12. The PIV standard consists of two parts: PIV - I and PIV – II. PIV – I satisfies the control objectives and meets the security requirements of HSPD 12, while PIV – II meets the technical interoperability requirements of HSPD 12. PIV-II specifies implementation and use of identity credentials on integrated circuit cards for use in a Federal personal identity verification system.

The Executive Office of the President, Office of Management and Budget (OMB), issued Memorandum M-05-24, Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, providing implementing instructions for the Directive (HSPD 12) and the Standard (FIPS 201). A schedule (timeline) for Agency Actions is provided within the memorandum. DHHS uses this memorandum as a basis for implementation while noting the importance of realizing that the use of standard identification does not replace current existing laws or OMB policy responsibilities; including the laws and policies governing personnel security, acquisition, and information technology security law.

The 2002 Federal Information Security Management Act (FISMA) does not permit waivers to the FIPS 201 standards.

3 ***APPLICABILITY***

FIPS 201, commonly referred to as "the Standard "is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2).

Current DHHS investigation requirements apply to all employees, intermittent, seasonal, per-diem, and temporary workers in either a single continuous or series of appointments. Applicability however, to other Department of Health and Human Services specific categories of individuals (e.g., short-term visitors (i.e. less than 6 months) guest researchers; volunteers; or intermittent, temporary or seasonal employees) is an OPDIV/STAFFDIV risk-based decision. Investigations are conducted in accordance with the risk/sensitivity of the position. Should individuals not meet either the criteria listed in existing HSPD 12 Directives or Standards, then the individual(s) concerned must follow any existing OPDIV/STAFFDIV policy and procedures for hosting, escorting, and allowing visitors (U.S. citizens or foreign nationals) access to DHHS owned and/or leased facilities. These individuals may be subject to PIV at the OPDIVS' discretion following a risk-based assessment. DHHS employees and Federal contractors who visit other DHHS campuses or areas of DHHS facilities for which they do not have electronic access authorization may be subject to the same OPDIV/STAFFDIV internal policies and procedures as visitors for accessing and being escorted in certain areas.

The HSPD 12 Program Office recommends that each OPDIV/STAFFDIV write, if not already in place, a policy that establishes procedures for visitors by type or category to include the applicability to HSPD 12. Most visitor practices usually address visitor types by placing them into three categories - Personal, Business and Working Visitors. Should an OPDIV/STAFFDIV require compliance with PIV of individuals listed as such in these "categories" of visitors and decide to require a background investigation predicated on internal policy or risk-based assessments, the OPDIV/STAFFDIV must then follow the processes outlined in *DHHS Office of Security and Drug Testing (OSDT) Personnel Security/Suitability Handbook, dated February 1, 2005,* where requirements for background checks for federal employees, contractors, and others employed for less than 6 months are listed. The only exception to existing DHHS policy is that all OPDIVS/STAFFDIVS must initiate the National Agency Check with Written Inquiries or other suitability or national security investigation prior to credential issuance. Identity credentials that are issued to individuals without a completed NACI or equivalent must be electronically distinguishable from identity credentials issued to individuals who have a completed investigation.

FIPS 201 also contains a special-risk security provision: "The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For those OPDIVS/STAFFDIVS with particularly sensitive OCONUS threats, the issuance, holding, and/or use of PIV credentials with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV credentials, the Secretary of DHHS may issue a select number of maximum security credentials that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, OPDIVS/STAFFDIVS should minimize the

number of requests for such special-risk security credentials so as to support inter-agency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, this need for this provision will be re-assessed as the standard undergoes the normal review and update process.

PIV Standards also apply to citizens of foreign countries who are working for the Federal government within CONUS and OCONUS. However, for those employees that are OCONUS, a process of registration and approval must be established using a method approved by the U.S Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander. These procedures may vary depending on the country.

Since Foreign National employees and contractors may not have lived in the United States long enough for a NACI to be meaningful, OPDIVS/STAFFDIVS should conduct an equivalent investigation, consistent with the operating divisions or staff divisions existing policy. Questions on conducting investigations of Foreign Nationals should be referred to the DHHS Director, Personnel Security & Drug Testing Office (OSDT).

4 ***SCHEDULES AND DEADLINES***

DHHS will create and implement a PIV I-compliant process no later than October 27, 2005.

DHHS will create and implement a PIV II-compliant system no later than October 27, 2006.

All DHHS employees with less than 15 years of Federal service as of October 27, 2005 will be identity proofed no later than October 27, 2007.

All DHHS contractors will be identity proofed no later than October 27, 2007.

All DHHS employees with more than 15 years of Federal service as of October 27, 2005 will be identity proofed no later than October 27, 2008.

All DHHS employees with less than 15 years of Federal service as of October 27, 2005 located in the National Capital Region (NCR), at Mission Critical Facilities (MCF), and in metropolitan areas will receive PIV II credentials no later than October 27, 2007.

All DHHS contractors located in the National Capital Region (NCR), at Mission Critical Facilities (MCF), and in metropolitan areas will receive PIV II credentials no later than October 27, 2007.

All DHHS employees with more than 15 years of Federal service as of October 27, 2005 located in the National Capital Region (NCR), at Mission Critical Facilities (MCF), and in metropolitan areas will receive PIV II credentials no later than October 27, 2008.

Employees and contractors not requiring a PIV II credential will receive another form of credential (TBD) no later than October 27, 2008.

All DHHS Logical Access Control Systems (LACS) will be upgraded to FIPS 201-compliant LACS no later than October 27, 2009.

All DHHS Physical Access Control Systems (PACS) will be upgraded to FIPS 201-compliant PACS no later than October 27, 2011.

5 ***ABBREVIATIONS***

CONUS: Continental United States (Including Alaska and Hawaii)

CHUID: Cardholder Unique Identifier

DA/OPPM: Departmental Administration/Office of Procurement and Personnel Management

DHS: Department of Homeland Security

DHHS: Department of Health and Human Services

e-QIP: Electronic Questionnaire for Investigations Processing

FIPC: Federal Investigations Processing Center

FIPS: Federal Information Processing Standard

FBI FP Check: FBI National Criminal History Fingerprint Check

FISMA: Federal Information Security Management Act

GSA: General Services Administration

HSPD: Homeland Security Presidential Directive

IDMS: Identity Management System

LACS: Logical Access Control System

MCF: Mission Critical Facility

NAC: National Agency Check

NACI: National Agency Check with Inquiries

NACIC – National Agency Check with Inquiries & Credit Check

NCR: National Capital Region

NIST: National Institute of Standards and Technology

OCIO: Office of the Chief Information Office

OCONUS: Outside the Continental United States

OIG: Office of the Inspector General

OMB: Office of Management and Budget

OPHEP: Office of Public Health Emergency Preparedness

OPM: Office of Personnel Management

OPM/NS BI: Office of Personnel Management or National Security Community Background Investigation

OSDT: Office of Security and Drug Testing

PACS: Physical Access Control System

PCI: Personal Identity Verification (PIV) Card Issuer

PIV: Personal Identity Verification

PIV I: Personal Identity Verification, Part I

PIV II: Personal Identity Verification, Part II

PKI: Public Key Infrastructure

SON: Submitting Office Number

TBD: To Be Determined

6 DEFINITIONS

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also "logical access control system" and "physical access control system."

Applicant – the individual to whom a PIV credential needs to be issued. The Applicant status only applies when an offer of employment is made and not before.

Approval Authority – is the individual who establishes the organizational chain of command within the Identity Management System (IDMS). This individual also manages the scope of the chain of trust between the enrollment process, the IDMS, card production and activation. This individual manages the entire IDMS and is responsible for designating those individuals who will perform the duties of the Employer/Sponsor. Additionally, the Approval Authority should make sure that *no single individual/role has the capability to issue a card without the participation of another individual and that there are at least two different individuals participating in the process at all times*. The Approval Authority should be responsible for validating and auditing all of the checks that are conducted by the IDMS.

Authentication - the process of establishing an individual's identity and determining whether individual Federal employees or contractors are whom they say they are.

Authorization - process of giving individuals access to specific areas or systems based on their authentication.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints, and facial images. A biometric system uses biometric data for authentication purposes.

Employer/Sponsor – is the individual who validates an Applicant's requirement for a PIV card and authorizes the Applicant's request. This function is normally associated with the Human Resources Office for Federal Employees and the Contracting Office for Contractors.

e-QIP Tracking Number – Number assigned by e-QIP to each SF-85 application. This tracking number must be written on the fingerprint card when it is submitted to OMB in order to bind the fingerprint card to the proper applicant.

FBI FP Check – Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI, and is the minimum requirement for provisional card issuance.

FD-258 – Contractor fingerprint card or Fingerprint Chart to accompany the NACI request when the individual to be investigated is a contractor (neither a Federal employee nor an applicant for Federal employment), or when agreed to by OPM-FIPC.

Identity Management System - one or more systems or applications that manage the identity verification, validation and issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing – the process of providing sufficient information (e.g., driver's license, proof of current address, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.

Issuing Authority (Issuer) – is the individual or entity that activates and issues a PIV card to an Applicant following the positive completion of all identity proofing, background checks, and related approvals. The Issuing Authority is responsible for ensuring that a one-to-one biometric check of the Applicant's enrolled fingerprint biometric image matches the fingerprint image at card issuance.

Logical Access Control System (LACS) – protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them. These systems may be built in to an operating system, application, or an added system.

Mission Critical Facility - a building or group of buildings in one geographical area, so vital to the United States and/or DHHS that the incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, DHHS mission accomplishment during exigent circumstances, or any combination thereof.

National Agency Check – the NAC is a part of every NACI. Standard NACs are the Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all new Federal employees and contractors consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

National Agency Check with Inquiries & Credit Check (NACIC) - the definitions statement under NACI with an additional requirement for a credit checks as stated for persons in Public Trust Positions (level 5C).

Public Trust Position – Positions (designated as Level 5 or 6) in which the incumbent's actions or inactions could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs; and positions in that the incumbents are being entrusted with control over information which the Department has legal or contractual obligations not to divulge.

Physical Access Control System (PACS) – protection mechanisms that limit users' access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV Authentication Certification Authority (CA) - is the Certification Authority that signs and issues the PIV Authentication Certificate of the Applicant.

PIV Card Issuer (PCI) – the individual or entity that issues an identity credential to an Applicant following the positive completion of all identity proofing, background checks, and related approvals. This role is normally associated with Badge or Credential Issuance. In most OPDIVS or STAFFDIVS it is a function of either Personnel or Physical Security. The PIV Card Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials. The PIV Card Issuer must be a government official or be designated in writing, as a PIV Card Issuer and the role of the issuer must be separated from that of the Registrar.

PIV II Credential – a government-issued credit card-sized identification that contains a contact and contactless chip. The holder's facial image will be printed on the card along with other identifying information and security features. The contact chip will store a PKI certificate, the CHUID, and a fingerprint biometric, both of which can be used to authenticate the user for physical access to federally controlled facilities and logical access to federally controlled information systems.

PIV Digital Signatory - is the entity that signs the PIV biometric and cardholder unique identifier (CHUID) of the Applicant.

PIV Registrar - the entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The "Registrar" role is normally associated with Personnel Security and Suitability or Human Resources. The Registrar must ensure that the minimum background investigations processes have taken place with positive results.

PIV Sponsor - the individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor must be a government official and be authorized in writing by the agency to request a PIV card. The PIV Sponsor requests the issuance of a PIV credential to the Applicant. The "Sponsor" role is normally associated with the Human Resources Center for Federal Employee Applicants and the Contracting Office for Contractors.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

Senior Agency Official for Privacy - Is the lead individual or entity for implementing PIV privacy policies and agency-specific policies and ensure that they are being applied and maintained in a consistent manner throughout every phase of the Federal Information Processing Standards Publication (FIPS-201) implementation (design, development, implementation, and post-implementation). This individual may not assume any other operational role in the PIV system (i.e., Registrar, Issuer, and Certifying Authority).

Standard Form (SF) 75 – is a standard form that is used by OPM as a request for preliminary employment data.

Standard Form (SF) 85 – is the minimum standard used for gathering information in the initiation of a background investigation. It is commonly referred to as the Questionnaire for Non-Sensitive Positions (NACI) - Level 1.

Standard Form (SF)-87 – Employee Fingerprint Card or Fingerprint Chart to accompany the NACI request when the individual to be investigated is a Federal employee or applicant for Federal employment.

Submitting Office Number (SON) – Number assigned by OPM to identify office that submitted the NACI request.

CHAPTER 2

PIV I

2.1 ***PIV I APPLICABILITY***

PIV I requires the implementation of registration, identity proofing, and issuance procedures in line with the requirements of FIPS 201. PIV I does not require the implementation of any new systems or technology.

PIV I only applies to new long-term (6 months or longer) employees and contractors who begin work at the DHHS on or after October 27, 2005. These individuals will have to follow the procedures outlined in section 4 below to apply for and receive their credentials. OPDIVS/STAAFFDIVS will continue to issue existing credentials under PIV I, but the process for application and issuance will change.

2.2 ***PRIVACY POLICY***

HSPD 12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. As such, DHHS agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in FIPS 201, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and OMB Memorandum M-03-22 (OMB322), as applicable.

Background investigation records are subject to the Privacy Act. OPDIVS/STAFFDIVS must ensure those records are:

- Secured against unauthorized access.
- Accessed by only those whose official duties require such access.
- Stored in a locked metal file cabinet or safe.

OPDIVS/STAFFDIVS must also:

- Establish procedures to allow employees or their designated representatives access to their own records, while ensuring that the records remain subject to agency control at all times.
- Ensure that those authorized to access personnel records subject to the Privacy Act understand how to apply the Act's restrictions on disclosing information from a system of records.
- See OPM's Guide to Personnel Recordkeeping, Chapters 1 and 6, at: http://www.opm.gov/feddata/recguide.pdf for instructions on proper safeguarding of personnel records.

2.3 ***NACI/NACIC/OPM/NS BI REQUIREMENTS***

A NACI is the minimum background investigation that must be performed for all individuals to whom this Directive applies, except when the position requires a higher-level OPM/NS BI. In such cases the OPM/NS BI shall be scheduled in lieu of the NACI.

These requirements may also be satisfied by locating and referencing a completed and successfully adjudicated NACI or other higher level OPM/NS BI. To locate and reference an already completed and successfully adjudicated NACI, contact the OPDIV/STAFFDIV human resources/or servicing personnel security and suitability offices. Procedures may vary across the Department and in some cases; responsibility may lie within the Human Resources Center (HRC) while in others it may reside with the OPDIV/STAFFDIV Personnel Security Office. If the Applicant indicates that he/she has already been awarded a specified level of security clearance based on a NACI/Other BI from previous employment, then the Applicant should be asked to present the corresponding certificate of clearance he/she was previously issued. Should he/she not have that specific certificate in possession, he/she should contact his/her previous employer's human resources or personnel security office to obtain a copy of or the original certificate. The certificate from the previous employer must have been issued no later than one year from the current date of inquiry. Finally, the OPDIV/STAFFDIV human resources center may meet the above requirements by completing the SF-75, Request for Preliminary Employment Data, Section K, Security Data, for federal employees transferring to the Department.

DHHS OPDIVS/STAFFDIVS human resources centers/or servicing personnel security offices are responsible for determining the position sensitivity designation for all positions and for ensuring that employees have the appropriate investigation commensurate with that determination. OPDIVS/STAFFDIVS must also ensure that periodic reinvestigations are scheduled as required. The DHHS OPDIV/STAFFDIV human resources center or personnel security office will submit the request for a NACI and the Standard Form 85 (SF-85) Questionnaire for Non-sensitive Positions, directly to the Office of Personnel Management (OPM) and make final PIV suitability determinations.

At a minimum, the FBI National Criminal History Fingerprint Check (FBI FP check) must be completed before the Registrar approves issuance of a provisional credential. The Registrar may issue a credential approval after the successful completion of a fingerprint check, however, the completion and successful adjudication of a full NACI is still required for all Applicants.

2.4 ***Public Trust Positions***

National Security positions requiring security clearances are limited at DHHS, but public trust responsibilities are much more prevalent and should be evaluated as the next step in the designation process. Although the public expects all federal employees to be trustworthy and honest, positions designated as Public Trust positions are those requiring a much higher degree of integrity with unwavering public confidence in the individual occupying the position. The sensitivity levels for Public Trust positions are as follows:

PUBLIC TRUST RISK LEVELS	
Risk Levels	**Minimum Investigation Required**
Moderate Risk Level 5	NACIC (NACI + credit check) MBI LBI
High Public Trust Level 6	BI

Public Trust positions include those involving policymaking, major program responsibility, and law enforcement duties. Also included are those involving access to or control of unclassified sensitive, proprietary information, or financial records, and those with similar duties through which the incumbent can realize a significant personal gain or cause very serious damage.

PRE-DESIGNATED LEVEL 5 PUBLIC TRUST POSITIONS	
$ Senior Executive Service (SES) Members $ Schedule C Appointees $ Administrative Law Judges $ Most Commissioned Corps Officers $ Employees required to complete OGE 450 and SF 278	$ General Schedule (GS)-13 to GS-15 Officials who are substantially involved in contracts, procurement, grants, or responsibilities involving a high risk for conflict of interest.

At DHHS, many of the employees, contractors, consultants, and experts who have access to computer information systems should be in positions designated as Public Trust. The public and the Department are put at risk if the incumbent does not meet the high standards of integrity and confidence required of those in Public Trust positions. OPDIV and STAFFDIV management must decide which of their positions have these enhanced public trust responsibilities, and thus should be designated as Public Trust positions. Management must further decide the relative degree of risk, moderate or high, inherent in these Public Trust positions so that they can assign a designated sensitivity level of 5 for moderate risk, or level 6 for high risk.

To promote consistency, effectiveness, and ease of operation within the Department, some personnel security and ethics program designations are being linked. The ethics program regulations require that employees in specific designated positions file an annual *Public Financial Disclosure Report Standard Form* (SF 278) or an annual *Confidential Financial Disclosure Report* (OGE 450) to ensure confidence in the integrity of the federal government by demonstrating that they are able to carry out their duties without compromising the public trust. By definition, these designated filers of an annual financial disclosure report occupy Public Trust positions and, for personnel security purposes, their positions shall be designated as Public Trust position Level 5 or 6, unless they meet the criteria for a National Security position, as stated in section 2.3.

Therefore, the ethics program designation should be used as the initial step in determining whether a position is a Public Trust position. If the incumbent of the position is required to file either annual financial disclosure report, then the incumbent is in a Public Trust position. The Department maintains lists of these designated positions and reviews them annually to assure that only positions that meet strict filing criteria are included. Although these positions are by definition "Public Trust positions," management still makes the most important personnel security decision in determining the relative risk level as either “moderate” or “high” (Level 5 or 6). This is the most important decision because the background investigation required of these two levels differs considerably in coverage and cost.

The required investigation of most entrants into a Level 5 Public Trust position is minimal, usually nothing more than a credit bureau check in addition to the regular required NACI investigation preformed on new hires. However, the credit check provides much information to aid management in deciding whether there is a risk in placing the individual in a Public Trust position. The required BI on an individual in a Level 6 position is a costly one with several years of coverage. Public Trust positions, following the designation criteria in the ethics program guidance, include positions

encumbered by the following officials: (not all-inclusive)

PRE-DESIGNATED LEVEL 6 PUBLIC TRUST POSITIONS	
$ OPDIV and STAFF DIV Heads $ Principal Deputy Assistant Secretaries	$ Institute and Center Directors $ Senior Information Systems Security Office

In addition to the "pre-designated" Public Trust positions, others meeting the definition and criteria must be designated as either a Level 5 or 6 Public Trust position.

NON PRE-DESIGNATED PUBLIC TRUST POSITIONS	
They should include positions having the following duties: $ Law Enforcement; $ Investigations; $ Audit; $ Security; $ Policymaking; $ Major program responsibility;	$ Access to sensitive, proprietary, or financial information, including access through, and/or control over, automated information systems (computer data systems); or $ Access to data covered by the Privacy Act.

In deciding if a Public Trust position has risks at the high level (6), remember that Level 6 requires a BI, and is best reserved for positions where information about the incumbent's entire background is very important, e.g., in law enforcement, investigator, and security positions. If in doubt, designate at Level 5, but require a LBI or another more thorough investigation above the minimum NACI and Credit.

High-Level PIV I Process

Applicants shall complete the appropriate questionnaire SF-85, SF-85P, SF-86 available on the OPM secure website. Completing e-QIP web-based security questionnaires will lead to improved processing time of all types of investigations and dramatically reduce the overall error and rejection rates of federal security questionnaires. Refer to section 2.5 below for specific step by step instructions on completing and adjudicating the NACI or NACIC.

2.5 ***REGISTRATION, IDENTITY PROOFING, & CREDENTIAL ISSUANCE***

The PIV I process contains critical roles associated with the identity proofing, registration, and issuance process. These roles may be ancillary roles assigned to personnel who have other primary duties, but no single individual may assume more than one of these roles in the process with the exception of the Adjudicator role. In some OPDIVS/STAFFDIVS, an individual may assume the role of the Adjudicator and Sponsor or both the Adjudicator and Registrar. The following roles shall be employed for identity proofing, registration, and issuance.

a. Roles and Responsibilities

(1) PIV Applicant

The Applicant is the individual to whom a PIV credential needs to be issued. Applicant responsibilities include:

- Complete required forms.
- Appear in person during various stages of the process.

(2) PIV Sponsor

The Sponsor is the individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. Sponsor responsibilities include:

- Coordinate initial registration activities.
- Validate and make copies of Applicant's identity source documents.
- Serve as intermediary between Applicant and Registrar.

(3) PIV Registrar

The Registrar is the individual responsible for identity proofing of the Applicant and coordinating NACI activities. The PIV Registrar provides the final approval for issuance of a PIV credential to the Applicant. Registrar responsibilities include:

- Register the applicant in e-QIP.
- Update OPF/Contract file.
- Approve or Deny Issuance of PIV card.

(4) Office of Personnel Management (OPM)

The OPM is responsible for conducting the appropriate investigation, for example: NACI, NACIC, BI and FBI FP Check.

(5) PIV Adjudicator

The PIV Adjudicator is the individual responsible for making a determination of whether or not the Applicant is eligible to receive a PIV Card, based on results obtained from OPM. Adjudicator responsibilities include:

- Confirm fingerprint check results.
- Adjudicate NACI and attempt to resolve issues.
- Update OPF/Contract file.

(6) PIV Issuer

The PIV Issuer is the individual who performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, fingerprint checks, and related approvals have been completed. Issuer responsibilities include:

- Confirm Applicant identification source documents.
- Capture photo and issue provisional card.

b. Registration, Identity Proofing, and Issuance Procedures

The following is a sequential list of steps to be following when applying for and issuing a credential that is compliant with the DHHS's PIV I identity proofing and registration process. This procedural outline provides a detailed description of logical flow, dependencies, and responsible parties.

(1) **Sponsor** – Send new hire package to Applicant and simultaneously notifies Registrar to grant Applicant access to e-QIP.

- Federal Employee New Hire Package includes: OF-306, Fair Credit Reporting Release, SF-85 or SF-87 (depending on previous service).
- Contractor New Hire Package includes: OF-306, Fair Credit Reporting Release, FD-258, and SF-85.

(2) **Registrar** – Register the Applicant in e-QIP. Notify Applicant of registration in e-QIP.

(3) **Applicant** – Complete OF-306, Fair Credit Reporting Release, and Fingerprint card as per agency instructions in new hire package from Sponsor.

(4) **Applicant** – After receiving notification from Registrar, complete SF-85 form online using e-QIP. Once SF-85 is completed, record e-QIP tracking number on fingerprint card (SF-87 for employees, FD-258 for contractors).

(5) **Applicant** – After completion of SF-85, appear in person in front of Sponsor with completed forms from new hire package, resume, and two identity source documents in original form. The identity source documents must come from the list of acceptable documents shown on Form I-9, OMB No. 1115-0136; Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID) card. OPDIVS/STAFFDIVS shall require Applicants who possess a current State

Drivers License or State Picture Identification Card to present that document as an identity source document before accepting other federal or state issued picture identification cards.

(6) **Sponsor** – Validate and copy source documents, collect Fair Credit Reporting Release, OF-306, resume, and fingerprint card from Applicant. Complete Sponsor section of DHHS Form TBD (PIV Request).

(7) **Sponsor** – Submit Fair Credit Reporting Release, OF-306, resume, fingerprint card, copy of source documents, and DHHS Form TBD (PIV Request) to Registrar.

(8) **Registrar** – Scan Fair Credit Reporting Release, OF-306, resume, and attach to Applicant's SF-85 in e-QIP. Update OPF/Contract file with original forms.

(9) **Registrar** – Send fingerprint card to OPM (make sure fingerprint card includes e-QIP Tracking Number).

(10) **OPM** – Run fingerprint check based on fingerprint card. Send results to Adjudicator (Identified by SON on e-QIP application).

(11) **Adjudicator** – Verify fingerprint check results received from OPM are successfully/unsuccessfully adjudicated and notify Registrar.

(12) **Registrar** – Review results of fingerprint check from Adjudicator. If approved, complete Registrar section of DHHS Form TBD (PIV Request) and send to Issuer. Send approval notification to Sponsor; go to step 14. If denied due to unusable fingerprints or incorrect identity, notify Sponsor; go to step 13.

(13) **Sponsor** – If fingerprint check was unsuccessful (unusable fingerprints, incorrect identity), determine whether to proceed with another fingerprint check or terminate the process.

(14) **Sponsor** – Contact Applicant after approval notification is received from Registrar and informs Applicant to appear in person in front of Issuer with identification source documents to receive credential.

(15) **Applicant** – Appear in person in front of Issuer and present state or federal ID.

(16) **Issuer** – Confirm Applicant's identity in person by verifying state or federal ID with source document information on DHHS Form TBD (PIV Request) received from Registrar.

(17) **Issuer** - Capture Applicant's photo and issue provisional credential. Complete Issuer section of DHHS Form TBD (PIV Request).

(18) **Applicant** – Complete Applicant section of DHHS Form TBD (PIV Request) acknowledging acceptance of credential and associated responsibilities.

(19) **Issuer** – Forward completed DHHS Form TBD (PIV Request) to Registrar.

(20) **Registrar** – Receive completed DHHS Form TBD (PIV Request) from Issuer and update OPF/Contract file with original completed DHHS Form TBD (PIV Request). Remove the provisional status of the credential.

(21) **OPM** – Conduct NACI and send final results to Adjudicator. Step 21 follows step 9 and can be completed concurrently with the activities in steps 10 through 20. (Applicants may be issued a provisional credential after the FBI FP Check portion of the NACI is completed and preliminary results are received at the OPDIV/STAFFDIV)

(22) **Adjudicator** – Adjudicate NACI according to the adjudication criteria listed below and in the DHHS-OSDT Personnel Security/Suitability Handbook. The adjudication process followed is found in 5 CFR Part 731-Suitability. The purpose of this part is to establish criteria and procedures for making determinations of suitability for employment in positions in the competitive service and for career appointment in the Senior Executive Service (hereinafter in this part, "competitive service") pursuant to 5 U.S.C. 3301 and Executive Order 10577 (3 CFR, 1954-1958 Comp. p.218). Section 3301 of title 5, United States Code, directs consideration of "age, health, character, knowledge, and ability for the employment sought." Executive Order 10577 directs OPM to examine "suitability" for competitive Federal employment. This part concerns only determinations of "suitability" based on an individual's character or conduct that may have an impact on the integrity or efficiency of the service. Determinations made under this part are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions made under Executive Order 10450 (3 CFR, 1949-1953 Comp. p.936), Executive Order 12968, or similar authorities. These same criteria are also used for the adjudication of Federal contractors. Upon completion of a successful NACI, the Adjudicator notifies the Registrar and Sponsor of the successful NACI:

(a) When adjudicating initial and continued eligibility to possess a credential, the Adjudicator shall make his or her determination based on the results of the FBI FP Check, NACI, other OPM/NS BI, or agency inquiry into misconduct.

(b) When making a PIV determination under (a) above, the Adjudicator must find whether or not the identity provided to the Sponsor and Registrar during the registration process is the Applicant's true identity. For applicants for employment and current Federal employees, the Adjudicator will consult with the applicant or employee's servicing Human Resources staff before making a final determination whether to deny or withdraw a credential.

(c) If the adjudication confirms the individual's true identity but reveals unfavorable information that involve criteria 1 through 8 below, an adjudication under Title 5, C.F.R. Part 731 shall be conducted. Title 5, C.F.R. Part 731 criteria are:

1 Misconduct or negligence in employment;

2 Criminal or dishonest conduct;

3 Material, intentional false statement or deception or fraud in examination or appointment;

4 Refusal to furnish testimony as required by §5.4 of Title 5, C.F.R.;

5 Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;

6 Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

7 Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;

8 Any statutory or regulatory bar, which prevents the lawful employment of the person, involved in the position in question.

(d) When making a suitability determination under Title 5 C.F.R. Part 731, the following factors shall be considered to the extent they are deemed pertinent to the individual case:

1 The nature of the position for which the person is applying or in which the person is employed;

2 The nature and seriousness of the conduct;

3 The circumstances surrounding the conduct;

4 The recency of the conduct;

5 The age of the person involved at the time of the conduct;

6 Contributing societal conditions; and

7 The absence or presence of rehabilitation or efforts toward rehabilitation.

(23) **Adjudicator** – Attempt to resolve any issues directly with Applicant.

(24) **Adjudicator** – If NACI adjudication is successful, notify Registrar, complete OFI-79A, store copy of OFI-79A in OPF/Contract file, and forward original OFI-79A to OPM; go to step 25. If NACI adjudication is unsuccessful, notify Registrar and Sponsor; follow appropriate OPDIV/STAFFDIV or DHHS procedures and policy.

(25) **Registrar** – If a Successful NACI is received from Adjudicator, remove provisional status from credential and update OPF/Contract file.

(26) **Registrar** – If NACI is unsuccessful, update OPF/Contract file and revoke credential.

(27) **Sponsor** – Notify Applicant of unsuccessful NACI, recover credential, and advise Applicant of appeal rights.

(28) **Applicant** – Appeal an unsuccessful Adjudication. (Optional)

c. ***Appeal Procedures for Denial of Credential***

In the event that Step 24 above is unsuccessful, the following procedure is to be followed:

(1) Appeal Rights for Federal Service PIV Applicants

When the PIV Adjudicator determines that a PIV Applicant has not provided his or her true identity during the registration process or is otherwise found unsuitable, and the determination results in a decision by the agency to withdraw an employment offer, or remove the employee from the federal service, the procedures and appeals rights of either 5 CFR Part 731, Subparts D and E (Suitability), 5 CFR Part 315, Subpart H (Probationary Employees), or 5 CFR Part 752, Subparts D through F (Adverse Actions) will be followed, depending on the employment status of the federal service applicant, appointee, or employee. Employees who are removed from federal service are entitled to dispute this action using applicable grievance, appeal, or complaint procedures available under Federal regulations, Departmental directives, or collective bargaining agreement (if the employee is covered).

(2) Appeal Rights for Contract PIV Applicants

Notice of Proposed Action – This criteria is subject to the compliance rules found in Federal Acquisition Regulation (FAR) Draft Interim Rule FAR Case 2005-015, Common Identification Standard for Contractors, specifically in that a written clause shall be added to the contract which specifically requires the contractor to comply with the PIV process for all affected employees in accordance with DHHS procedures. When the PIV Adjudicator determines that a PIV Applicant has not provided his or her true identity or is otherwise not suitable to be employed in the current or applied for position, e.g. an unsuccessful adjudication, the PIV Adjudicator shall provide the individual reasonable notice of the determination including the reason (s) the individual has been determined to not have provided his or her true identity or is otherwise unsuitable. The notice shall state the specific reasons for the

determination, and that the individual has the right to answer the notice in writing. The notice shall inform the individual of the time limits for response, as well as the address to which such response should be made.

Answer - The individual may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

Decision - After consideration of the determination and any documentation submitted by the PIV Applicant for reconsideration of the initial determination, the OPDIV Head/STAFFDIV Office Director or his/her delegated designee will issue a written decision, which informs the PIV Applicant/Respondent of the reasons for the decision. The reconsideration decision will be final. The United States Government will not be responsible for payment of services while the Applicant is not working on the designated contract or services to the OPDIV/STAFFDIV.

2.6 EXPIRATION DATE REQUIREMENTS

All credentials issued by the DHHS must have an expiration date printed on the card. The expiration date for all credentials must be 5 years or less from the date of issuance for Federal employees; 1 year or less for contractors.

All existing credentials in the NCR, MCF, and metropolitan areas must be replaced with PIV II credentials no later than October 27, 2008. Employees with less than 15 years of Federal service as of October 27, 2005 and all contractors must have their credentials replaced with PIV II credentials by October 27, 2007. Employees with more than 15 years of Federal service as of October 27, 2005 must have their credentials replaced with PIV II credentials by October 27, 2008.

All credentials issued to applicable employees and contractors outside the NCR, MCF, and metropolitan areas must be replaced with PIV II credentials by October 27, 2007.

2.7 CASES WHERE PIV I DOES NOT APPLY

HSPD 12 Implementation guidance for Federal Departments and Agencies does not apply to occasional visitors to Federal facilities to whom you would issue temporary identification. It also does not apply to “Government corporations” as defined by title 5 U.S.C. 103(1), however these corporations are encouraged but not required to implement this directive.

DHHS has identified several cases where the PIV I process does not need to be followed to secure a credential. OPDIVS/STAFFDIVS may choose to implement stricter requirements at their own discretion following a risk-based assessment of their facility requirements.

a. Replacement Credentials

Replacement credentials are to be issued when an employee or contractor credential is lost, damaged, stolen, or expired.

Sponsors are required to complete the Sponsor section of DHHS Form TBD (PIV Request) and check the replacement card box. Sponsor and Applicant will follow pre-existing credential issuance procedures for obtaining a replacement credential; these procedures will vary by agency and facility.

b. Temporary Credentials

Temporary credentials are authorized as a part of PIV however they must be clearly identified as such and issued only to those with a successfully completed NACI. For Identity credentials that are issued to individuals without a completed NACI or equivalent, these credentials must be electronically distinguishable (i.e. information is stored inn the data on the card) from identity credentials issued to individuals who have a completed investigation. Section 2.2 of the Standard has been revised to clarify for the initial credential issuance; only the fingerprint check must be completed. The Department of Commerce (DOC) will provide the electronic format for this information.

c. Visitor Credential

OPDIVS/STAFFDIVS shall follow existing procedures for issuing visitor badges. Visitor badge procedures will vary by OPDIV and facility.

2.7 CONTRACTING IMPACTS

All contractors must abide by the identity proofing and registration requirements outlined in section 2.5 of this document. DHHS contract statements of work must indicate that:

All long-term contractor employees must go through the identity proofing and registration process,

All incumbents must be successfully identity proofed and have a successfully adjudicated NACI or OPM/NS BI to serve on the contract.

Certain PIV language must be implemented in all contracts. Please refer to FAR Case 2005-015, "Secure and Reliable Identification of Contractor Employees" for specific language.

2.8 AUDIT & RECORDS MANAGEMENT

The HSPD 12 Program Office within the Office of the Assistant Secretary for Administration and Management has responsibility for auditing identity proofing and registration records. As such, all OPDIVS/STAFFDIVS should be prepared for such reviews.

OPDIVS/STAFFDIVS must comply with the appropriate policies and directives related to "Records Management", for the creation, maintenance, use, and disposition of all records associated with the PIV process.

2.9 USE OF APPROVED FORMS

To comply with the Paperwork Reduction Act (PRA) of 1995, all OPDIVS/STAFFDIVS are required to use OMB approved forms throughout the identity proofing and

registration process (i.e. SF-85). Most of these forms are standard Federal government-wide forms that have been available for several years. In addition to the government-wide forms, the DHHS is creating an additional PIV specific form that will fulfill the information gathering requirements of the PIV program. The following is a list of approved forms for use in the PIV I process:

DHHS Form TBD, PIV I Request & Issuance Approval Form

Fair Credit Reporting Release

FD-258, Fingerprint Chart for Contractor Position

OF-306, Declaration for Federal Employment

OPM OFI-79A, Report of Agency Adjudicative Action on OPM Personnel Investigations

Standard Form (SF) 85, OPM Questionnaire for Non-Sensitive Positions. (To be completed using e-QIP)

Standard Form (SF) 87, Fingerprint Chart for Federal Position

2.10 PHYSICAL ACCESS CONTROL SYSTEMS (PACS)

PIV I does not address PACS. However, in preparation for PIV II, OPDIVS should evaluate existing PACS during FY 06 as follows:

a. Continued Use of Existing PACS

FIPS 201 mandates that all DHHS controlled facilities use access control, a guard, or some other method to control access to our facilities. Physical access control will continue to be managed at the OPDIV or facility level, however, the DHHS long term strategic plan is to implement a FIPS 201-compliant enterprise-wide PACS infrastructure by October 27, 2009 in order to distribute and revoke identity information based on the PIV process.

b. Upgrading Existing PACS

The DHHS plan calls for the implementation of FIPS 201-compliant PACS by October 27, 2011. If any agency/DHHS facility plans to replace or install a physical access control system they must contact OPHEP Physical Security to coordinate the installation, receive the latest version of GSA approved HSPD 12-compliant systems and a list of vendors who have installed DHHS systems successfully. The system that is chosen must be compatible with the DHHS Identity Management and Access control enterprise.

c. Purchase of New PACS

There are numerous options available to install fully compliant low cost access control, (from simple card readers, to fully functional access control portals to automatically grant physical access to DHHS facilities). OPDIVS/STAFFDIVS must comply with GSA HSPD 12 Memorandum regarding the Acquisitions of Products and Services for Implementation of HSPD 12. OPDIVS/STAFFDIVS must only purchase systems from the GSA list of approved products and ensure

the systems will be compatible with the DHHS enterprise-wide PACS centralized infrastructure. Contact DHHS-OPPM Physical Security or the OPDIV Facilities Management Office to discuss compliant options.

2.11 LOGICAL ACCESS CONTROL SYSTEMS (LACS)

PIV I does not address LACS. However, in preparation for PIV II, OPDIVS/STAFFDIVS should evaluate existing LACS during FY 06 as follows:

a. Continued Use of Existing LACS

PIV I does not require the issuance or use of PIV II credentials with a contact chip. As such, DHHS will continue to issue existing ID badges to all employees and contractors. The DHHS does not currently have a significant smart card implementation, and existing LACS do not support the use of PIV II credentials at an enterprise level. OPDIVS must continue to integrate applications requiring authentication with the DHHS eAuthentication service, and continue to use the existing credential assurance levels as defined in OMB Memorandum M-04-04, and "DHHS E-Authentication Service" policy.

b. Upgrading Existing LACS

OPDIVS/STAFFDIVS may have to replace existing computer equipment as the technology reaches the end of its lifecycle. Any changes or upgrades must be made in accordance with OPDIV/STAFFDIV policy. The DHHS Information and Technology Transformation and all proposed DHHS information management and technology investments must be evaluated to ensure they align with DHHS business goals, objectives of the DHHS E-Government mission, and integrate with and not duplicate DHHS and government-wide initiatives. Therefore, all upgrades to existing LACS must be approved by the DHHS Chief Information Officer (CIO) to ensure the products will be compatible with the DHHS's card issuance and management system. DHHS plans to implement a FIPS 201-compliant enterprise-wide LACS infrastructure by October 27, 2009. OPDIVS/STAFFDIVS should check the status of emerging DHHS standards for peripheral devices, keyboards, card readers, etc. before making purchases.

c. Purchase of New LACS

Beginning in October 2006, PIV II credentials containing a contact chip and digital certificate will be issued based on the schedule outlined above in section 4. OPDIVS/STAFFDIVS will make risk-based decisions on what level of assurance they will require for access to their information systems. Based on these assurance level decisions, the purchase of card readers, and biometric readers may be required. The DHHS Information and Technology Transformation and all proposed DHHS information management and technology investments must be evaluated to ensure they align with DHHS business goals, objectives of the DHHS E-Government mission, and integrate with and not duplicate DHHS and government-wide initiatives. Therefore, the CIO must approve all new LACS purchases. All purchases approved by the CIO must be of products included on the GSA schedule of FIPS 201-compliant products and vendors. Products on the GSA schedule have gone through the necessary testing to ensure compliance with the technical and interoperability requirements of PIV II.

CHAPTER 3

PIV II

3.1 ***PIV II OVERVIEW***

PIV II is the implementation phase that meets the technical interoperability requirements of HSPD 12. Specifically, PIV II addresses the technical infrastructure for providing interoperable credentials for federal employees and contractors. All authentication mechanisms described in FIPS 201 are to be met with the use of integrated circuit cards.

FIPS 201 describes minimum technical requirements for the PIV II credential. These requirements include interfacing specifications, cryptographic specifications, PKI and certificate specifications, card topology specifications, and biometric data specifications. The PIV card issued will be used to control physical access to all federally controlled facilities and logical access to all federally controlled information systems through a contact or contactless interface.

For PIV II, DHHS will implement a system-based model with increased functionality to improve efficiency and accuracy in processing PIV applications. PIV II will include three new logical subsystems:

- PIV Front-End Subsystem - PIV Card, card and biometric readers, and personal identification number (PIN) input device. The PIV cardholder interacts with the front-end subsystem to gain physical or logical access to the desired Federal resource.

- PIV Card Issuance and Management Subsystem - the components responsible for identity proofing and registration, card and key issuance and management, and various repositories and services required as part of the verification infrastructure.

- Access Control Subsystem – the physical and logical access control systems, protected resources, and authorization data.

DHHS will implement PIV II using a risk-based, phased approach according to the schedule outline in the INTRODUCTION, section 4. This Departmental Handbook will be updated with more specific details about the PIV II systems and processes by October 27, 2006.

3.2 ***PIV II APPLICABILITY***

PIV II applies to all applicable long-term federal employees and contractors based on risk assessments. PIV II applies to the following facilities and information systems:

a. Facilities

Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a Federal department or agency.

Federally controlled commercial space shared with non-government tenants.

Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.

b. Information Systems

Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3502(8)).

Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, (44 U.S.C. §3544(a)(1)(A).

Applicability for employee or contractor access of Federal systems from a non-Federally controlled facility (e.g. researchers' up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on risk.

4.1 ***TRAINING***: The following link is for the PIV –I roles and responsibilities training module:

http://www.vodium.com/goto/blm/hspd12.asp

CD's will be available shortly. Future training modules will be posted to the USALearning.Gov web site.

4.2 ***WHERE TO GET ASSISTANCE***: In the interim period you may contact either the Director, HSPD 12 Program Office at (202) 690-7431 or on e-mail at zjt8@cdc.gov or mario.morales@hhs.gov.

4.3 ***REPORTING REQUIREMENTS***

OPDIVS/STAFFDIVS are required to submit quarterly and annual reports on their PIV card programs to ensure controls are in place for tracking all PIV credentials. Agencies must submit the following reports to HSPD 12 Program Office within 15 days of the end of each quarter and the fiscal year:

a. Number of PIV credentials issued during designated period

- Cardholder Name
- Card Identifier
- Card Issuance Date
- Card Expiration Date

b. Number of PIV credentials cancelled during designated period

- Cardholder Name
- Card Identifier
- Card Cancellation Date
- Reason For Cancellation (Retirement, Termination, Damage, etc.)

c. Number of PIV credentials replaced during designated period

- Cardholder Name
- Old Card Identifier
- New Card Identifier
- Date Replaced
- Reason For Replacement

4.4 ***PIV I PROCESS FLOW DIAGRAM***: TBD

4.5 ***HSPD 12 DOCUMENT***

Homeland Security Presidential Directive/HSPD 12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting,

and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH